Claims

[c1] 1. A method for disabling a virus in a computer, the method comprising the steps of: (a) identifying a system object in the computer that is required by the virus; and (b) storing an access control entry (ACE) in an access control list (ACL) for said system object, wherein said ACE specifies an entity and a permission needed by said entity to access or execute said system object, and said ACE further specifies that said entity is denied said permission, thereby disabling the virus by denying said entity future ability to access or execute said system object.

[c2] 2. The method of claim 1, wherein said system object in the computer is not the virus itself.

[c3] 3. The method of claim 1, wherein said ACE specifies a said entity including all users and groups of the computer, thereby disabling the virus by denying any said entity future ability to access or execute said system object.

[c4] 4. The method of claim 1, wherein said ACE specifies a said permission including all access to said system object, thereby disabling the virus by denying said entity any future ability to access or execute said system object.

[c5] 5. The method of claim 1, wherein the computer employs a registry, and the method further comprising editing said registry

to disable automatic execution of said system object.

[c6] 6. The method of claim 5, further comprising monitoring said registry for edits that will cause execution of said system object, and performing the method if any said edits are detected.

[c7] 7. The method of claim 1, further comprising: (c) rebooting the computer after said step (b), thereby terminating any present execution of the virus.

[c8] 8. The method of claim 7, wherein said step (c) is initiated by a command remotely communicated to the computer via a network.

[c9] 9. The method of claim 7, further comprising determining whether said ACE for said system object stored in said step (b) has remained unchanged after said step (c), and repeating the method if not.

[c10] 10. A method for disabling a process in a computer, the method comprising the steps of: (a) identifying a system object in the computer that is required by the process; and (b) storing an access control entry (ACE) in an access control list (ACL) for said system object, wherein said ACE specifies an entity and a permission needed by said entity to access or execute said system object, and said ACE further specifies that said entity is denied said permission, thereby disabling the process by denying said entity future ability to access or execute said system object.

[c11] 11. The method of claim 10, wherein said system object in the computer is the process itself.

[c12] 12. The method of claim 10, wherein said ACE specifies a said entity including all users and groups of the computer, thereby disabling the process by denying any said entity future ability to access or execute said system object.

[c13] 13. The method of claim 10, wherein said ACE specifies a said permission including all access to said system object, thereby disabling the process by denying said entity any future ability to access or execute said system object.

[c14] 14. The method of claim 10, further comprising: (c) rebooting the computer after said step (b), thereby terminating any present execution of the process.

[c15] 15. The method of claim 14, wherein said step (c) is initiated by a command remotely communicated to the computer via a network.

[c16] 16. The method of claim 14, further comprising determining whether said ACE for said system object of said step (b) has remained unchanged after said step (c), and repeating the method if not.

[c17] 17. The method of claim 10, wherein said system object is not initially present in the computer, and further comprising: creating

an instance of said system object; and storing said instance of said system object in the computer at one or more storage locations, wherein said step (b) stores a said ACE in a said ACL for each instance of said system object, thereby inoculating the computer against execution of the process by preventing storage of other instances of said system object in said storage locations.

[c18] 18. The method of claim 17, wherein said ACE specifies a said entity including all users and groups of the computer, thereby disabling the process by denying any said entity future ability to store said system object in said storage locations.

[c19] 19. The method of claim 10, wherein an authority has deemed the process inappropriate for use by said entity.

[c20] 20. The method of claim 19, wherein the process is inappropriate because improper use will impair conventional use of the computer.

[c21] 21. The method of claim 19, wherein the process is inappropriate because use by said entity will violate a policy set for use of the computer.

[c22] 22. An article of manufacture made by the method of claim 1.

[c23] 23. An article of manufacture made by the method of claim 10.

[c24] 24. A computer program, embodied on a computer readable storage medium, for disabling a virus in a computer, comprising:

a code segment that identifies a system object in the computer that is required by the virus; and a code segment that stores an access control entry (ACE) in an access control list (ACL) for said system object, wherein said ACE specifies an entity and a permission needed by said entity to execute said system object, and said ACE further specifies that said entity is denied said permission, thereby permitting disabling the virus by denying said entity future ability to access or execute said system object.

[c25] 25. The computer program of claim 24, wherein said code segment that identifies said system object in the computer permits specifying a said system object that is not the virus itself.

[c26] 26. The computer program of claim 24, wherein said code segment that stores said ACE permits specifying a said entity including all users and groups of the computer, thereby permitting disabling the virus by denying any said entity future ability to access or execute said system object.

[c27] 27. The computer program of claim 24, wherein said code segment that stores said ACE permits specifying a said permission including all access to said system object, thereby permitting disabling the virus by denying said entity any future ability to access or execute said system object.

[c28] 28. The computer program of claim 24, wherein the computer employs a registry, and further comprising a code segment that

edits said registry to disable automatic execution of said system object.

[c29] 29. The computer program of claim 28, further comprising a code segment that monitors said registry for edits that will cause execution of said system object, thereby permitting detection of any said edits.

[c30] 30. The computer program of claim 28, further comprising a code segment that reboots the computer, thereby permitting terminating any present execution of the virus.

[c31] 31. The computer program of claim 30, wherein said code segment that reboots is initiate-able by a command remotely communicated to the computer via a network.

[c32] 32. The computer program of claim 30, further comprising a code segment that determines whether said ACE for said system object stored by said code segment for storing has remained unchanged after rebooting.

[c33] 33. A computer program for disabling a process in a computer, the method comprising the steps of: a code segment that identifies a system object in the computer that is required by the process; and a code segment that stores an access control entry (ACE) in an access control list (ACL) for said system object, wherein said ACE specifies an entity and a permission needed by said entity to access or execute said system object, and said

ACE further specifies that said entity is denied said permission, thereby permitting disabling the process by denying said entity future ability to access or execute said system object.

[c34] 34. The computer program of claim 33, wherein said code segment that identifies said system object in the computer permits specifying a said system object that is not the process itself.

[c35] 35. The computer program of claim 33, wherein said code segment that stores said ACE permits specifying a said entity including all users and groups of the computer, thereby permitting disabling the process by denying any said entity future ability to access or execute said system object.

[c36] 36. The computer program of claim 33, wherein said ACE specifies a said permission including all access to said system object, thereby disabling the process by denying said entity any future ability to access or execute said system object.

[c37] 37. The computer program of claim 33, further comprising a code segment that reboots the computer, thereby permitting terminating any present execution of the process.

[c38] 38. The computer program of claim 37, wherein said code segment that reboots is initiate-able by a command remotely communicated to the computer via a network.

[c39] 39. The computer program of claim 37, further comprising a code segment that determines whether said ACE for said system object stored by said code segment for storing has remained unchanged after rebooting.

[c40] 40. The computer program of claim 33, wherein said code segment that stores said ACE is a first code segment, and further comprising: a code segment that creates an instance of said system object; and a second code segment that stores said instances of said system object in the computer at one or more storage locations, wherein said first code segment that stores particularly stores a said ACE in a said ACL for each instance of said system object, thereby permitting inoculating the computer against the process when said system object is not present in the computer.

[c41] 41. The computer program of claim 40, wherein said ACE specifies a said entity including all users and groups of the computer, thereby permitting disabling the process by denying any said entity future ability to store said system object in said storage locations.

[c42] 42. A system for disabling a process in a computer, comprising: means for identifying a system object in the computer that is required by the process; and means for storing an access control entry (ACE) in an access control list (ACL) for said system object, wherein said ACE specifies an entity and a permission

needed by said entity to access or execute said system object, and said ACE further specifies that said entity is denied said permission, thereby permitting disabling the process by denying said entity future ability to access or execute said system object.

[c43] 43. The system of claim 42, wherein said system object in the computer is the process itself.

[c44] 44. The system of claim 42, wherein said ACE specifies a said entity including all users and groups of the computer, thereby permitting disabling the process by denying any said entity future ability to access or execute said system object.

[c45] 45. The system of claim 42, wherein said ACE specifies a said permission including all access to said system object, thereby permitting disabling the process by denying said entity any future ability to access or execute said system object.

[c46] 46. The system of claim 42, further comprising means for rebooting the computer after said means for storing has stored said ACE, thereby permitting termination of any present execution of the process.

[c47] 47. The system of claim 46, wherein said means for rebooting is operable in response to a command remotely communicated to the computer via a network.

[c48] 48. The system of claim 46, further comprising means for

determining whether said ACE for said system object stored by said means for storing has remained unchanged after said means for rebooting has rebooted the computer.

[c49] 49. The system of claim 42, wherein said means for storing said ACE is a first means for storing and said system object is not initially present in the computer, and further comprising: means for creating an instance of said system object; and second means for storing said instance of said system object in the computer at one or more storage locations, wherein said first means for storing particularly stores a said ACE in a said ACL for each instance of said system object, thereby permitting inoculating the computer against the process when said system object is not present in the computer.

[c50] 50. The system of claim 39, wherein said ACE specifies a said entity including all users and groups of the computer, thereby permitting disabling the process by denying any said entity future ability to store said system object in said storage locations.